State of Missouri

CYBERSECURITY TASK FORCE ACTION PLAN

Missouri Office of Administration
Information Technology Services Division (ITSD)
Missouri Office of Cyber Security

Submitted to Governor Jeremiah W. (Jay) Nixon
12/29/2016

Table of Contents

Letter from State of Missouri Cybersecurity Task Force 2

State of Missouri Cybersecurity Task Force Members 3

Executive Summary 4

Survey 4

Common Themes with Recommendations 5

Five Foundational Pillars 7

1 - WORKFORCE DEVELOPMENT 7

Summary 7

Identified Gaps with Recommendations 7

2 - INFORMATION SHARING AND AWARENESS 12

Summary 12

Identified Gaps with Recommendations 12

3 - INCIDENT RESPONSE 14

Summary 14

Identified Gaps with Recommendations 14

4 - TRAINING AND EXERCISES 19

Summary 19

Identified Gaps with Recommendations 19

5 - HARDENING CRITICAL INFRASTRUCTURE 21

Summary 21

Identified Gaps with Recommendations 21

Conclusion 28

PRIMARY RECOMMENDATIONS 28

State of Missouri Cybersecurity Task Force Message

December 29, 2016

Governor Jeremiah W. (Jay) Nixon
State Capitol Building, Room 216
Jefferson City, MO 65101

Dear Governor Nixon and the Citizens of Missouri:

The State of Missouri Cybersecurity Task Force was created to identify cybersecurity best practices and a path forward for the state to work offensively against a growing number of cyber threats. The task force, comprised of representatives from state, county and city governments; law enforcement entities; private industry; and higher education and K-12 institutions, among others, focused on five foundational pillars:

1) Information Sharing and Awareness, including sharing past experiences and information about current and emerging threats and industry best practices;
2) Training and Exercises, with an emphasis on sharing expertise and experience on tools proven most effective in detecting and defending against the growing number of cyber events;
3) Workforce Development, including strategies for educating the current and future cybersecurity workforce;
4) Hardening Critical Infrastructure such as the electrical grid with an emphasis on ensuring continuity of services; and
5) Incident Response: with an emphasis on swift and effective coordinated response to cyber threats.

Information for the following action plan was gathered during task force meetings, at the Governor's Cybersecurity Summit, and from responses to a cybersecurity readiness survey which was distributed to organizations across the state.

Maintaining the status quo on cybersecurity responsiveness is simply not an option as the world around us continues to advance and the threats become more and more serious. Combining our cyber defense efforts among all sectors will provide a means to strengthen each sector's defense capabilities. The knowledge gained from this cybersecurity initiative has helped to make recommendations on ways to coordinate efforts between the public and private sectors to strengthen our statewide cybersecurity posture.

Thank you for your dedication to this very important issue. If we continue to work together, we can all do our part to help fight cyber criminals and keep Missourians' data safe.

Sincerely,

2016 State of Missouri Cybersecurity Task Force members

State of Missouri Cybersecurity Task Force Members

STATE

1 - State of Missouri, ITSD	Rich Kliethermes
2 - State of Missouri, ITSD	Mike Roling
3 - State of Missouri, ITSD	Steve Siegler

K-12

4 - MoreNet (K-12)	Gloria Stephenson
5 - Park Hill	Dr. Jeanette Cowherd

HIGHER ED

6 - Southeast Missouri State	Dr. Vijay Anand
7 - Missouri S&T	Bruce McMillin
8 - STL Community College	Craig Chott

LAW ENFORCEMENT

9 - Highway Patrol	Patrick Woods
10 - SEMA	Dawn Warren, Ron Walker
11 - National Guard	Maurice McKinney, Aaron Larimore
12 - Kansas City PD	Mike Grigsby
13 – NFCA, KCPD	Troy Campbell

LOCAL GOVERNMENT

14 - Cape Girardeau County	Charlie Herbst
15 - City of Springfield	Jeff Coiner

SECURITY

16 - World Wide Technology	Chris Konrad, Rick Dudeck
17 - REJIS	Eric Gorham
18 - FireEye	Thomas MacLellan
19 - AT&T	David Hulsey
20 - Jack Henry	Beth Young

PRIVATE

21 - Cerner	Don Kleoppel
22 - Wipro	Ashish Kumar, James Goss
23 - KCPL	Charles King, Gary Johnson
24 - Black & Veatch	Brandon Dunlap
25 - Central Bank	Dan Westhues
26 - Carrie's Hallmark	Carrie Tergin (Jefferson City Mayor)
27 - Boeing	Andrew Dolan, Shawn Lorimer

Office of Administration Commissioner Doug Nelson
Office of Administration Communications Director Ryan Burns

EXECUTIVE SUMMARY

In June of 2016, the Commissioner of the State of Missouri's Office of Administration, with support from Governor Nixon, formed the State of Missouri's first ever Cybersecurity Task Force. The Task Force, consisting of over 30 members from local government, law enforcement, business, higher education and K-12 institutions, was created to identify actionable recommendations and coordinate efforts between public and private sectors across the State of Missouri.

The plan before you is the compilation of many discussions and feedback from numerous businesses, governments, and schools across the State of Missouri on different ways organizations can improve their cybersecurity posture.

The Task Force was divided into subgroups to tackle the five identified cybersecurity pillars:

1. **Information Sharing and Awareness**, including case studies and information sharing on current and emerging threats and industry best practices;
2. **Training and Exercises**, with an emphasis on sharing expertise and experience on tools proven most effective in detecting and defending against the growing number of cybersecurity events;
3. **Workforce Development**, including strategies for educating the current and future cybersecurity workforce;
4. **Hardening Critical Infrastructure**, such as the electrical grid with an emphasis on ensuring continuity of services; and
5. **Incident Response**, with an emphasis on swift and effective coordinated response to cybersecurity attacks.

SURVEY

The Task Force distributed a survey to multiple industries that included agriculture, education, energy, financial, government, healthcare, information technology (IT), and law enforcement. These industries varied by employee sizes from 1 to over 20,000. The purpose of this survey was to have an understanding on industry readiness, maturity, and awareness on various cybersecurity topics. The survey was sent to multiple industry associations, and the results were anonymously collected. Forty-eight different organizations completed the survey with most of them falling under government and education (Figure 1). The survey results are used in this document to quantifiably provide evidence about the current state of cybersecurity within Missouri and assist with the recommendations.

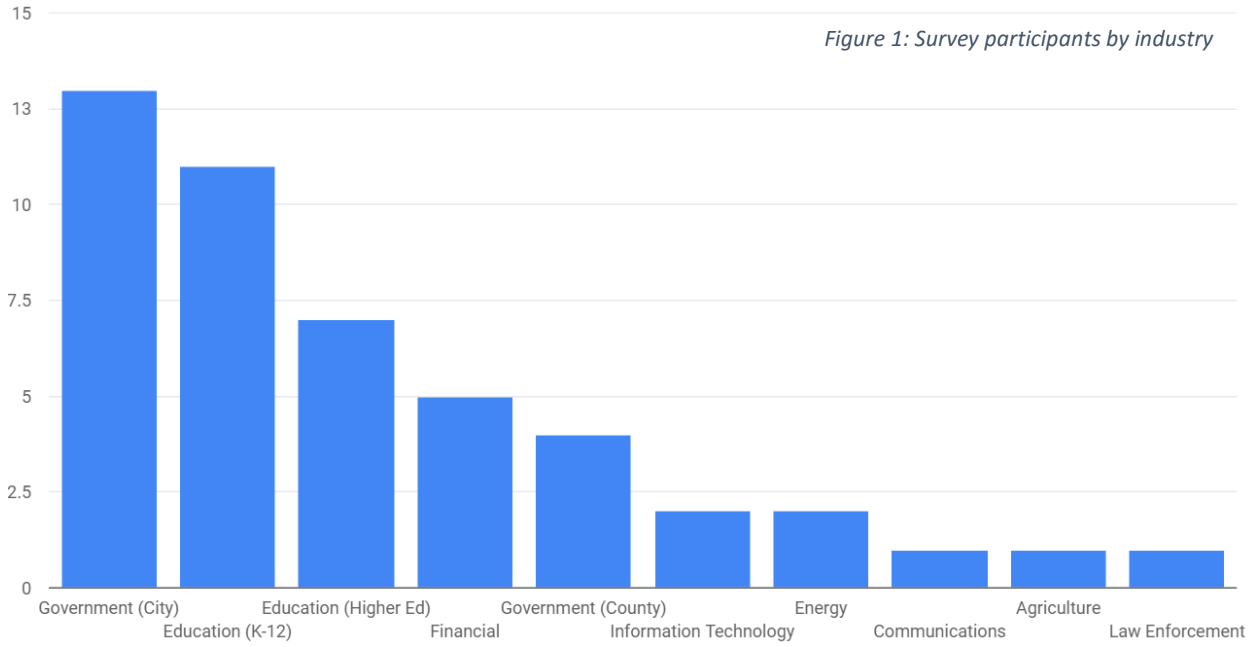

Figure 1: Survey participants by industry

COMMON THEMES WITH RECOMMENDATIONS

While compiling all of the various recommendations, several themes surfaced above the rest. These themes hold value in all of the five pillars and in many cases are requirements for success:

- **Awareness** - Throughout all of these pillars, awareness is the primary driver that brings about great change. Awareness spans vast topics across cybersecurity, Information Technology (IT), and business as a whole. Being aware of critical organizational functions and understanding the techniques, tactics, and procedures of threat actors that want to cause harm gives decision makers the information they need to mitigate cybersecurity risk effectively. When awareness is interwoven within the day-to-day operations of an organization it becomes a part of its culture and empowers employees to become the first and last line of defense. In other words, awareness expands cybersecurity beyond just the cybersecurity team and gives key stakeholders the information they need to protect their organization. Awareness isn't something that can be bought; it takes due care and diligence from the very top to make awareness thrive within an organization.

- **Resources** – Many organizations around the State of Missouri lack the necessary resources to properly protect themselves from cybersecurity attacks. Small governments and school districts across the state are struggling to find the budget and workforce capable of mitigating the threats they face on a daily basis. Many of these organizations are refreshing aging critical infrastructure with systems that are Internet enabled. And with the explosion of the Internet of Things (IoT), the risk and the attack surface will only increase. Multiple times throughout 2016, we have seen small city and county governments fall victim to either cybersecurity attacks or poor cybersecurity hygiene which costs local tax payers tens of thousands of dollars and delays services. The State of Missouri is poised and willing to assist local governments tactically with various security services already deployed within state government. The State of Missouri could also assist other organizations on a voluntary basis within its statutory authority. As can be seen in Figure 2, over 90% of the Cybersecurity Task Force survey participants have some interest in state provided solutions.

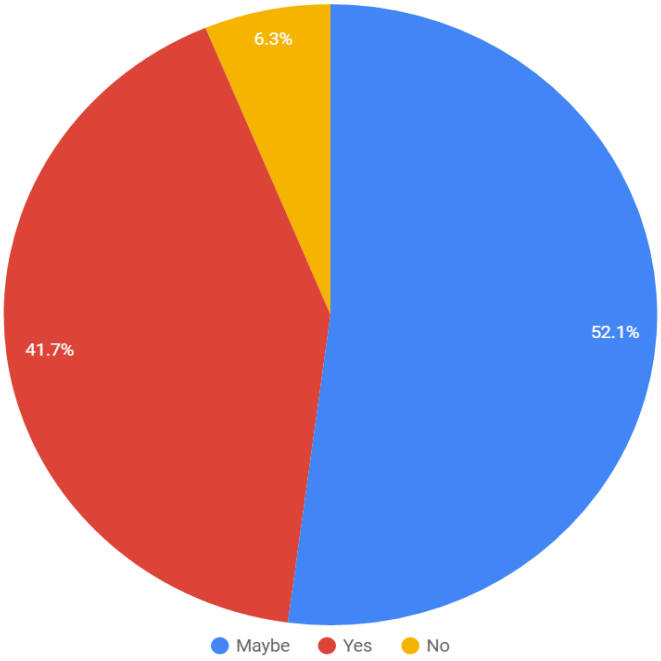

Figure 2: Survey participants interest in state provided solutions

Larger Missouri organizations with a dedicated cybersecurity budget and workforce are doing a good job at keeping up with the adversary. Many of the organizations share intelligence with each other and with their industry community for even greater protection. Money and cybersecurity talent does not grow on trees; it either takes a cataclysmic cybersecurity event or strong leadership to spur a cybersecurity program. Mature organizations are poised to assist those that are struggling with finding resources. In addition, having a Missouri Information Sharing and Analysis Center (ISAC) dedicated to the threats Missouri organizations face would greatly reduce the risk for participating organizations.

The talent problem can be addressed in multiple ways. For starters, strengthening science, technology, engineering, and mathematics (STEM) within our schools by showing students how 'cool' IT and cybersecurity

fields are through cybersecurity competitions and other hands-on experiences. Many Missouri-based higher education institutions have outstanding cybersecurity curriculums that can be leveraged even further through a proposed centralized cybersecurity institute. The institute, if created, could also be a center for certifications, act as an interface between industries and education, and share general information about cybersecurity.

Identified Cybersecurity Gaps and Recommendations

1 - WORKFORCE DEVELOPMENT

Summary

Careers in cybersecurity are some of the fastest growing and highest demand job opportunities available. The U.S. Department of Labor (DOL) groups cybersecurity specialists within the category of "Information Security Analysis, Web Developers, and Computer Network Architects". The outlook for this group is promising. DOL expects 22 percent growth within the next decade, which is considered faster than average. Demand for information security analysts is expected by DOL to be "very high". They justify this by pointing to the increased frequency and sophistication of cyber-attacks. Based on these expected workforce requirements, survey questions were formulated to understand the needs of different entities in Missouri.

The survey questions developed for workforce development are the following:

1. What are the strengths employers see in current cybersecurity professionals and what are the weaknesses that employers wish addressed?
2. Would you utilize a cybersecurity institute in the state of Missouri that offered certifications for your employees? Would you find benefit if they offered directive communication for handling current threats, and networking opportunities with other businesses about cybersecurity?
3. How much are internships/co-ops experience important before joining the workforce? Do the companies have internship/co-op programs?
4. What are the preferred methods of educational/training delivery, i.e. distance streaming video, offline training, on campus training, site-specific courses, massive open online courses (MOOC)?
5. Which security certifications do employers seek in a cybersecurity professional? How important are those certifications to employers?
6. How can industry participate in competitions from K-12 to college?
7. What programming languages are necessary in your workplace that are not being currently offered in the education system?

Based on the survey results, discussions amongst subject matter experts, and guidance from other major organizations, the following gaps were identified with the recommendations.

Gap #1: Centralized structure for educational outcomes

Surveys and analysis by the team indicated there was a lack of cybersecurity awareness and available cybersecurity talent at all levels in many organizations. When talent is available, many organizations cannot afford dedicated cybersecurity professionals.

Currently, cybersecurity in the classroom is still maturing. While there are some great higher education programs across the state, they vary in focus. This can be confusing for students who want to choose cybersecurity as a career, as well as for businesses in Missouri that hire cybersecurity professionals directly out of college.

Academic Designations and Accreditations: Educational entities such as technical institutes, community colleges, four-year colleges, and research universities can provide Center for Academic Excellence standards as highlighted by the National Security Agency/Department of Homeland Security (NSA/DHS). These standards prescribe particular sets of topics on security and privacy that accredited institutions must deliver to specific audiences. The state currently has one Center of Academic Excellence in Information Assurance which functions at the graduate and professional continuing education level. The Computing Accreditation Commission (CAC) of ABET, Inc. is proposing to include cybersecurity as a specific part of the CAC Computer Science Program Criteria for four-year and above universities to follow who wish to be

accredited. Apart from these, there is the cybersecurity education project that also attempts to frame an accreditation mechanism.

Research: The state has one Center of Academic Excellence in Information Assurance Research with additional research activities at other universities focused on cybersecurity research. The research activities at these schools can result in outreach to support state cybersecurity needs through federal programs such as the Industry/University Cooperative Research Centers (I/UCRC) which partner industry and government with research programs. It is difficult for industries to learn about research capabilities statewide and determine how this research capability can be used to assist specific cybersecurity issues. There are also few terminal degree granting universities in Missouri, which forces students to go to other terminal degree granting universities in other states.

Recommendation: Cybersecurity Institute

To address the gaps noted above, the establishment of a cybersecurity institute for the State of Missouri is proposed. This centralized body could serve as a partnership between education, industry and government to identify relevant training, research, information sharing activities and communication to help citizens identify relevant cybersecurity topics that people, businesses and organizations need. This institute thereby would act as a facilitator of cybersecurity related educational and workforce development endeavors between different entities within the State of Missouri. The different roles this institute would assume are:

Academic Coordination: The institute would provide a clearing house and expertise for those institutions seeking cybersecurity designations and accreditation. This is a challenging task and the existing accredited institutions can provide assistance through the institute to share best practices and facilitate developing curriculum that meets national standards.

Research Coordination: The institute would provide "one stop shopping" for businesses and governments seeking solutions to cybersecurity issues. Federal support can enhance state support through the Federal I/UCRC programs and others to bring together industry, education, and government.

Research Funding: This proposed institute would become the conduit to fund cybersecurity research in the state. State and national funding for cybersecurity topics is critical for researchers within the state of Missouri. This institute can become the facilitator between public and private entities to encourage research for the most pressing topics that impact the State of Missouri.

Scholarships: Another important role of such an institute would be to hand out scholarships to keep students in the state. This is an important undertaking since scholarships attract student's interest and provide incentives for high-achieving students to stay in the state. The National Science Foundation Scholarship for Federal Service (SFS) is a program designed to encourage bright students to pursue education and enter government service (both state and federal).

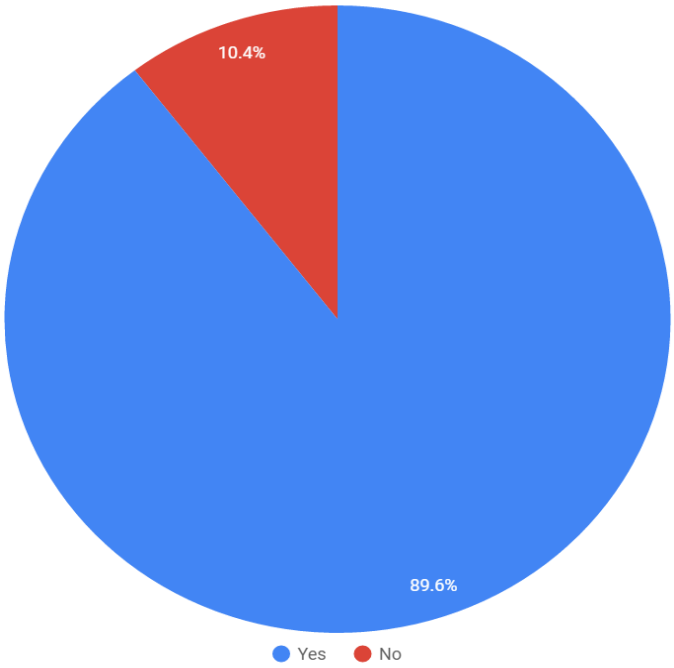

Figure 3: Survey participants that would utilize cybersecurity institute.

Career Services: This institute would also become a facilitator for industries that seek individuals to hire; everyone from interns to full-time hiring. Partnering with the Federal Office of Personnel Management (OPM), the SFS program virtually guarantees job placement.

Apart from the different funding sources, state and national funding for cybersecurity topics is critical for researchers within the state of Missouri. This institute can become a facilitator between public and private entities to encourage research for the most pressing topics that impact the State of Missouri.

Gap #2: K-12 educational short falls

In today's society, cybersecurity continues to be a growing concern. From the individual to corporate perspective we are all seeing an increase risk of intrusion. This risk has thrust cybersecurity into the forefront of available career opportunities. According to St. Louis Community College's State of St. Louis STEM Workforce Report, in 2013 there were over 23,000 STEM jobs available, but only 2,000 jobseekers looking for those opportunities. It is also predicted that there will be over 1 million jobs available by the year 2020 to protect our nation's cybersecurity infrastructure.

A critical part of our success to fulfill future needs is by engaging the youth of today to become interested in STEM. There are many great examples of cities taking initiative, and their success has been found on two fronts, curriculum adoption and competition engagement.

One of the important findings within our survey was the lack of trained personnel in cybersecurity.

The educational standards for the state do not have any requirements for curriculum focused on computation. Currently the state is doing some level of participation in cybersecurity training. Several schools are currently participating in Project Lead the Way's Computer Science program with some degree of success. The adoption rate has been high, but schools are experiencing some challenges to implement.

- The cost may be prohibitive to some small and rural schools in the state.
- The ownership of the teaching becomes hard due to instructors with little knowledge or background on the subject.
- Many districts are categorizing cybersecurity curriculum into the business department.
- It doesn't align with the critical certifications employers are looking for when hiring.

The need for educators holding degrees in computing is not one of the areas of acceptance by American Board for Certification of Teacher Excellence (ABCTE). The closest one comes to a computation related field of study is that of tech and engineering in the traditional route. The pipeline of educators teaching computing is therefore limited in the state.

Recommendation: Modification of High School Curriculum

Currently there are no guidelines for cybersecurity related studies within the K-12 system. It is therefore our recommendation that the State of Missouri and the Department of Elementary and Secondary Education (DESE) modify the curriculum to add cybersecurity related studies in the K-12 framework as has been accomplished by few other cities and states. In concurrence with the previous recommendation for creating a cybersecurity institute, the state can provide resources to partners who will advocate for furthering curriculum adoption and partnering with interested schools. The institute can work closely with DESE to ensure a minimum viable product will be created in which all schools can easily incorporate courses into their curriculum. We would also recommend collaborating with the Cyber Texas Foundation to provide subject matter expertise to the state. Their support will expedite the process.

Recommendation: Cybersecurity studies specialization for teachers

The lack of trained personnel teaching cybersecurity studies is a major gap and this requirement needs to be met to support the changes to the K-12 curriculum to incorporate cybersecurity studies. Currently no such specialization exists in the teacher training programs and degrees and hence our recommendation is to create a standalone specialization in cybersecurity studies to the educational training program.

Gap #3: Importance of Internship Opportunities

Internships offer numerous benefits to both the student and the offering organization. The student obtains real world, hands-on experience within cybersecurity, and in many cases, the intern will go on to work within the offering organization. In regards to the survey responses, 34 of the 48 responses indicated that internships and internship opportunities are important in their industry. However, there are not enough internship opportunities available for the demand.

Recommendation: Centralized Internship Registry

The State of Missouri should provide a centrally coordinated registry to connect cybersecurity internship opportunities with potential interns.

Recommendation: Provide Private Sector Internship Incentives

The State of Missouri should provide the private sector with incentives that encourage them to provide more internship opportunities, which would also be included in the state's internship registry system.

Gap #4 Industry Certifications

Only 18 of the 48 responses indicated the importance of industry certifications. We feel this is an artificially low number considering the lack of private sector survey participants. Scanning daily job listings would indicate that the importance of industry-recognized certifications is much higher in reality.

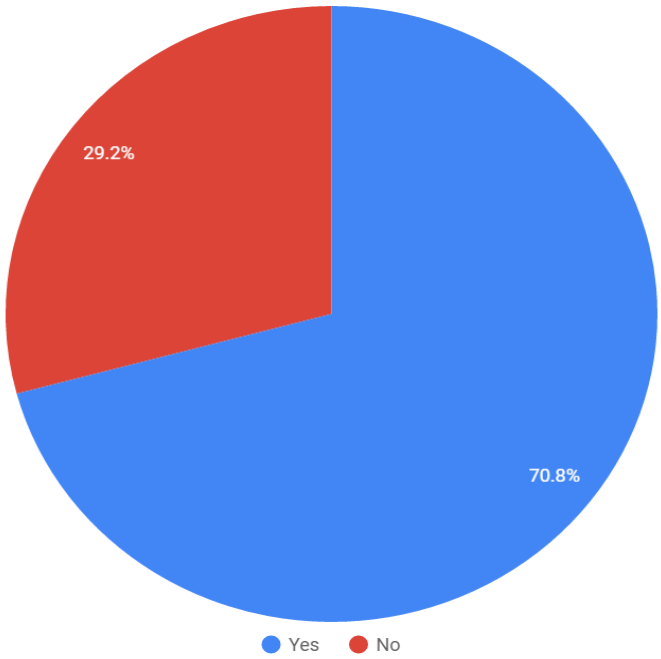

Figure 4: Survey participants' response to the importance of internships.

Recommendation: Provide Certification Cost Reimbursements

The State of Missouri should provide cost reimbursements (in whole or partial) to those who obtain industry-recognized certifications in their field. This would encourage continued education, professional development, and adherence to the codes of ethics of the certification organizations.

Gap #5: Competitions and Student interest

Competitions provide students goals and necessary excitement which keeps them focused on a particular topic. Students typically spend time beyond classwork on the technical topics which foster learning that a typical coursework cannot provide. Competitions that require group interactions help students develop skills in group dynamics. Another outcome of such competitions is the technical writing that the student needs: from resume building to writing basic reports of incidents that they encountered during a competition. Within a curricular program, competitions have a symbiotic relationship that enables student to maintain interest and focus, allows faculty to interact with students as participants, and gives students the ability to hone their skills within a classroom environment. There are various competitions in which students at different levels can participate. Businesses understand the need of such competitions and they sponsor many of these initiatives. In addition, businesses recruit from the competitions.

Recommendation: Funding for Competition

The recommendation of this group is provide some funding to allow students to compete at all such competitions. Currently no explicit funding exists and creation of such a fund would foster more students to compete, elevating the quality of the competition and creating a large competent knowledge base.

Recommendation: Funding for creation and maintenance of a Cybersecurity Stadium

The State of Missouri should also provide funding for creating and maintaining a cybersecurity stadium that would allow competitors to practice for the competition's goals and the hosting the competitions. Currently one such infrastructure exists where students compete and have had a pretty good track record regionally. This infrastructure can be enhanced to host simultaneous virtual competitions for all types of students.

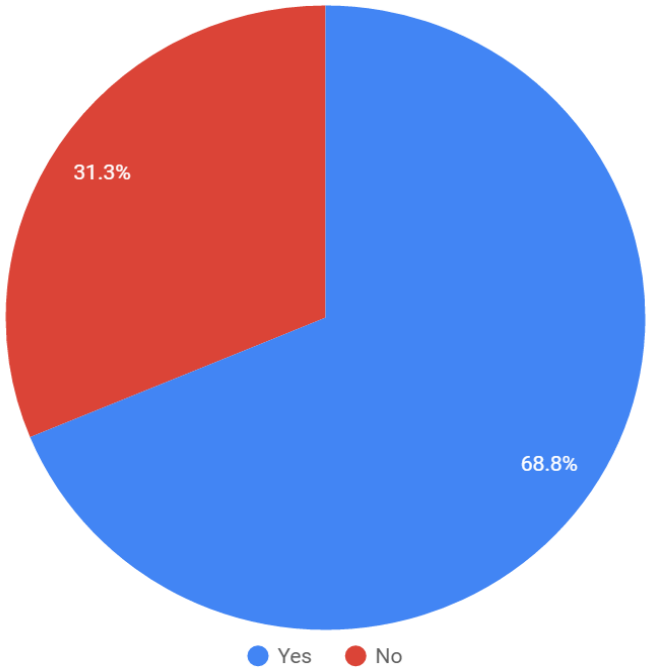

Figure 5: Survey participants' response to the importance of cybersecurity competitions.

2 - INFORMATION SHARING AND AWARENESS

Summary

Information sharing has become paramount in protecting organizations both big and small. The sharing of actionable information has not only been proven to thwart bad actors attempting to steal data and disrupt organizations, but also raises cybersecurity awareness to a new level by better understanding the current threat landscape. While some of the larger organizations in Missouri coordinate with industry ISACs and receive timely information about current threats, smaller organizations tend to be left out in the dark. Smaller organizations, including small businesses, schools, hospitals, banks, local government, and local utilities, deliver many essential services to Missouri citizens. It is vital that timely, actionable threat information gets shared with these organizations.

Gap #1: Communication of current threat landscape

From the survey results, there was a marked difference between governmental entities and private sector in support from senior leadership, which could mean that management might not be aware of what the current threat landscape looks like and what risks the organization might be facing. Smaller organizations were more likely to rely on email to disseminate information, while larger organizations also had newsletters and blog posts and were more likely to hold security briefings.

Recommendation: Sharing current cybersecurity threats

The State of Missouri should organize security workshops to educate people on the current threat landscape. These workshops should be held throughout the population centers of the state. A Missouri based cybersecurity ISAC, in coordination with the various fusion centers, should be created to assist in the decimation of information seen across the state and country. The ISAC could also play other roles such as coordinating with other ISACs and organizations.

Gap #2: Cybersecurity Initiatives

When asked on the survey what was lacking in order to execute cybersecurity initiatives, most organizations indicated that strategies around successful mitigations and detection were needed. There was also a need for more intelligence information, especially around threats and trends in security. The need for indicators of compromise was lower than expected. This seems to imply that people are getting lots of indicators from other sources and that they need help either implementing detection strategies around that data and maybe contextual threat information is needed. It may also mean that the survey participants may not have the capability to ingest or produce cybersecurity indicators.

Recommendation: Best practices help for "big picture"

There are many best practice documents available to help organizations with strategies around mitigations and detection. It might be helpful to have a list of available links to all the best practice documents, like National Institute of Standards and Technology's (NIST) Cybersecurity Framework, Internal Revenue Service's (IRS) Publication 1075, Federal Information Security Management Act (FISMA), Center for Internet Security (CIS) Top 20, and others. It might also be useful to hold round table discussions within like industries/sectors for real time discussions on how each organization is handling their own security.

Recommendation: Security workshops on current cybercrime trends

Quarterly meetings could be held to discuss current trends in cybersecurity crime. Different sectors could be tapped to help generate the content. Meetings could be held online so travel could be eliminated.

Gap #3: Sharing indicators of compromise

While most people implied that they get enough indicators from other sources, they are willing to share indicators with others, as long as it is properly anonymized. Unfortunately, most people indicated that email was their preferred

method of sending/receiving indicators. This method does not scale well and can cause a delay as people cut/paste indicators into local solutions. There is also a greater chance of errors being introduced. Automation is needed for scalability.

Recommendation: Training around STIX/TAXII or other threat intel automation

In order to be effective, indicators need to be shared in an automatic way. This will reduce delays in processing the data; no need to wait on a person to read/act on an email message and will reduce the accidental introduction of errors in the data caused by cut/paste. The State of Missouri currently operates a TAXII server and could be used to facilitate threat intel sharing. Training could be provided on installing TAXII servers and how to connect TAXII servers together for information sharing or accounts could be given on the state's TAXII server for smaller organizations.

Gap #4: Senior Leadership is not engaged

About half of the respondents indicated that their senior leadership was not engaged in cybersecurity, which could indicate a lack of awareness of current threats and the need for security solutions.

Recommendation: Security briefings for executives

The State of Missouri could organize security workshops to educate people on the current threat landscape. It might also be useful to send out quarterly newsletters that could be shared with senior management. This could be divided by sector. A separate survey to executives could also be distributed to establish why they are not involved; is it a time factor or perhaps they don't understand the need?

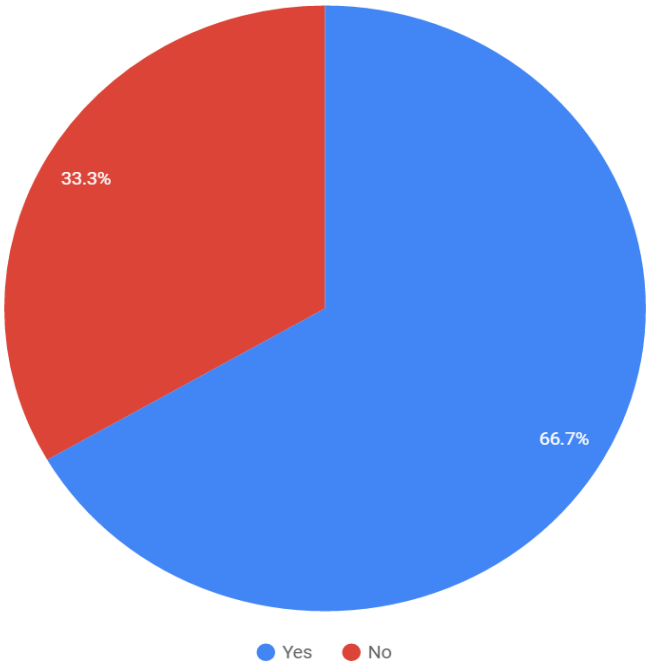

Figure 6: Survey participants that have an end user awareness program

Gap #5: Security Awareness training

One third of the survey respondents reported that they have no end user awareness training. Of those that do have awareness training, almost everyone has modules for Phishing, Social Engineering and Email. The larger organizations also include modules on handling PII, web security, security while traveling and WiFi/mobile security.

Recommendation: State wide purchasing contract

The State of Missouri could investigate the feasibility of creating a statewide purchasing contract so smaller organization could have security awareness training at reduced rates. This will bring training to organizations that don't currently have training and allow others to expand their offerings.

Recommendation: Create a speaker's bureau

The State of Missouri could run a speakers' bureau. Many organizations would like an expert to give presentations to employees or members (such as Rotary, Kiwanis or Lions Clubs). By creating a speakers' bureau, trainers could sign up to give presentations in their area of the state. The state could also create and maintain standard slide decks so all presenters would be giving the same information and sharing a consistent security message.

3 - INCIDENT RESPONSE

Summary

Managing the response to a cybersecurity incident has quickly become as critical to operating a successful IT organization as implementing the technology itself. The impact of cybersecurity incidents is not only felt by IT employees. Today the impact is felt by everyone from the employees taking payments at the cash register to the executives making strategic decisions in the boardroom.

When organizations witness headlines about the failures of other companies, they must be more diligent in creating a plan that will help them reduce the risk to their business.

The Missouri Cybersecurity Task Force identified five gaps that are preventing higher levels of adoption and support for cybersecurity incident response plans. These gaps include:

1. **Communication**
2. **Legal/Legislative/Liability concerns**
3. **Cybersecurity response structure**
4. **Response plans are not documented or exercised**
5. **Awareness and the need for a plan isn't recognized or understood**

Gap #1: Communication

Communication is a vital part of responding to a cybersecurity incident. Depending on the size and scope of the incident, multiple parties may need to be involved in the conversation regarding how the event impacts the operations. Knowing which organizations or agencies need to be in the loop can be confusing, especially in the midst of trying to recover from a large scale incident.

Questions will arise during the response such as: How did this happen? Are we at risk for more exposure to the threat? What do we need to do to fix this and get back to normal operations? How much can we share? Which stakeholders need to know? Do we need to involve local, state or federal law enforcement? How do we respond to media questions? How often do we need to provide updates and what channels of communication should we use to do so?

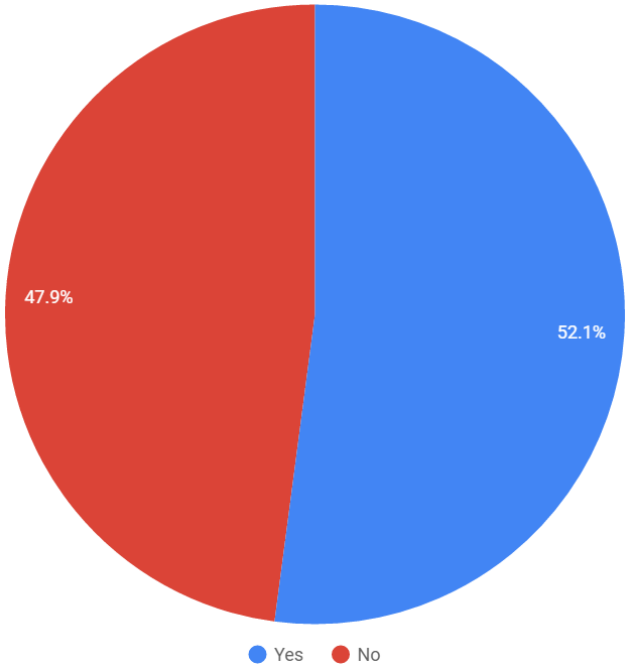

Figure 7: Survey participants with an incident response plan

Communication immediately after a cybersecurity incident can make or break an organization. The following recommendations are suggested to help bridge the communication gap during an incident response.

Recommendation:

Develop a template of communication considerations during an incident response

A key to communication during a cybersecurity incident response is to notify the appropriate authorities, employees, customers and other stakeholders. The development of a template with a list of questions that may arise during an event will help organizations think through information that will need to be communicated prior to and/or during an incident. The template could also help with the dissemination of consistent and timely information to the appropriate stakeholders.

Recommendation: Provide resources that can assist organizations with all aspects of communication when they have been impacted by a cybersecurity incident

Many organizations may not have cybersecurity professionals that are able to respond to or provide guidance during a cybersecurity event. Experienced resources that are well-versed in the communication requirements during a cybersecurity incident could assist those organizations. This would give them much needed information such as who to involve and how to deal with specific security issues.

Gap #2: Legal/Legislative/Liability concerns

There are a number of legal, legislative and liability concerns that must be considered when responding to a cybersecurity event. If the organization has cybersecurity insurance, what does it cover? Does the organization have or need mutual aid agreements in place to receive assistance from a government agency? What agencies or companies have the ability to respond to specific types of incidents? Are corporations willing to share assessment information with the state? Would they be willing to provide expertise if needed? Are there legislative changes that are needed in order to alleviate concerns with liability or the sharing of information? What level of funding is required to address assistance for cybersecurity responses?

Recommendation: Review the legal requirements and issues of liability regularly in order to keep up with changes in technology and security concerns

Each state has its own laws regarding data breach requirements. The Missouri State Statutes are defined in section 407.1500.1. They define a "breach of security" or "breach", as “unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.”

While this definition works for personal information, how would a breach of critical infrastructure in a utility power plant, computer systems used in manufacturing, or other computerized equipment sometimes referred to as the Internet of Things (IoT) be defined?

Legislation needs to be reviewed regularly to ensure that State and Federal laws are not creating hurdles for companies or government agencies to overcome as they assist in responding to a cybersecurity concern.

Recommendation: Remove legal and liability barriers that prevent mutual aid in cybersecurity incident response

Companies and government agencies may be reluctant to request assistance from other organizations unless a formal agreement is in place to protect personal information or forensic findings regarding a breach or outage from a cybersecurity incident.

Barriers that may prevent mutual aid during a cybersecurity incident response to any organization should be removed wherever possible. Cybersecurity laws should not prevent but enable the sharing of information with other entities that may be able to assist or benefit from the information by preventing similar events from occurring.

Gap #3: Cybersecurity Response Structure

Each business or government agency and the technology critical to their operations are unique. Cybersecurity incidents are also unique events. As such, the response needs to be adaptable and scalable to the size and scope required.

Attempting to think through each of these scenarios can be an overwhelming task for any organization. Assistance from others that have been through cybersecurity incidents is invaluable. Utilizing existing emergency management practices can also be helpful.

The following recommendations are intended to assist in bridging the gaps of the cybersecurity response structure for large or small companies and agencies alike.

Recommendation: Define your Mission and Scope

To begin with, it is best to define your incident response structure in terms of who you are serving, the scope of your services, the authority from which you intend to operate, the organization affiliation and the domain you are responsible for. All of these elements, as well as many others necessary for defining the structure of an incident response program, can be found in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2350. While you may not be trying to build a nation-level Computer Security Incident Response Team (CSIRT), this document format is useful in ensuring that you have aligned with well-established practices and that you have not left out key principles and functions that your own organization, or others requesting your assistance, would rely upon.

Recommendation: Plan for a Dynamic and Flexible Structure

Not all incidents are handled in quite the same way, and circumstances will dictate the proper structure for any given scenario. Depending upon whether your response team is responding to an internal incident or assisting another organization, such as a client or supplier, the reporting chain will vary. In some cases, your own Incident Commander may be subordinate to another organization such as law enforcement or even an external public relations firm, depending on the nature of the incident. Your own reporting structure should include provisions for ensuring communications within your organization are handled in a consistent manner while still allowing for the appropriate and timely interface with the external parties also involved. By creating these channels of communication before they are needed, and properly exercising them, you can build a confident and capable team that can be relied upon to support the internal functions as well as providing crisp execution for external stakeholders.

Recommendation: Organize According to Function

While smaller organizations will not likely be able to staff and maintain a full-time CSIRT capability, with many individuals performing these functions only in times of crisis, it is important to assign roles and capabilities according to the flows of information. These functions can be broken down into the following tiers:

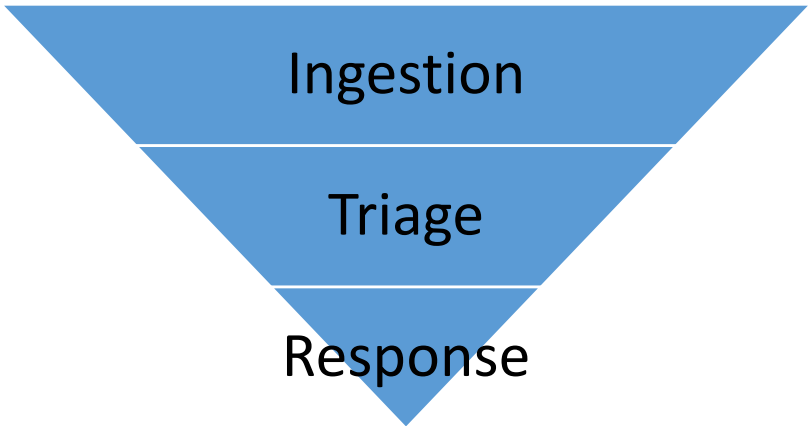

Figure 8: IETF RFC 2350 incident response tiers

The ingestion function is the primary contact point with internal and external stakeholders and may include the service desk, human resources or other parties not directly within your sphere of control. However, all channels for receiving first contact about an incident should know how to direct to the appropriate response team member(s) to ensure that the incident is logged and routed correctly to the triage phase. Often times, the triage phase is a member of the information security team or a knowledgeable member of IT. Once the proper severity is assigned, then the response phase can begin, also likely including outsiders to the core IT or security function, such as human resources (if the

incident included possible malicious inside actors), marketing and communications (in the event of press or customer notifications) and often legal (to determine scope of potential liability and possible insurance actions.

Gap #4: Cybersecurity plans are not documented or exercised

There's an old saying among sports teams, "we play how we practice." This is certainly true for responding to a large scale cybersecurity incident. It could end up like any sporting event with professionals on offense and amateurs on defense. The results wouldn't be pretty. So why aren't more organizations investing the time and effort it takes to document the response plan and practice responding to an incident? Are they expecting IT to handle it? Do they think they can operate for long periods of time without technology? Today, the likelihood of operating any business or government agency without technology today is unrealistic.

The following recommendations are intended to assist with documenting and exercising cybersecurity response plans.

Recommendation:

Provide guidance for organizations to develop comprehensive incident response plans

An unfortunate reality is that many organizations will never think about how they would respond to a cybersecurity incident until they fall victim to an attack. Even those that have a basic response plan are missing critical components that hinder the incident response teams in the initial hours of the response. This recommendation is to provide organizations with guidance necessary to ensure that those elements critical to facilitating an effective incident response are included in an organization's incident response plan. Examples of these critical elements are system documentation, critical personnel contact information and system classifications/prioritization.

Recommendation:

Provide opportunities and templates in order to facilitate incident response exercises

Organizations that have been proactive in incident response planning still cannot account for the unknown. An important aspect of incident response planning is to exercise plans, examine results and adjust the plan accordingly. This recommendation is to provide organizations with guidance on building efficient incident response exercises that can uncover unknown aspects of incident response and allow incident response plans to be adjusted to become more comprehensive. By providing templates, organizations can develop scenarios that are likely to impact a particular industry or sector and perform an effective exercise. This recommendation is also aimed at providing guidance on performing quick exercises that can be performed on a regular interval basis. Opportunities should be afforded for organizations to come together and perform exercises off-site with the opportunity for review and input from cybersecurity experts onsite.

Gap #5: Awareness and the need for a plan is not recognized or understood

Raising awareness of cybersecurity concerns and the need for a documented, exercised incident response plan is critical. From the C-suite to public relations, legal and risk management, and certainly IT and operational aspects of any business, awareness is critical in gaining the attention required to make sure a cybersecurity response plan is in place.

While the numbers of recent events that have been publicized have helped raise awareness and concerns outside of the IT organization, there is a common feeling lacking in most organizations that "cybersecurity is a shared responsibility."

Recommendation: Raise awareness of the importance of an incident response plan at all levels of the organization

One of the most difficult tasks for senior leadership is to raise awareness across their enterprise regarding cybersecurity activities and what cybersecurity means to an organization. In order to accomplish such a daunting task, here are some options and ideas that may assist in raising cybersecurity awareness.

- Develop additional cybersecurity training based off of recent cybersecurity incidents
- Exercise employees with cybersecurity activities such as implementing an e-mail phishing scenario, internal social engineering attempts etc.
- On the spot "Face-to Face" praises and corrections at the supervisory level
- Supervisors being held accountable for all staff failures to accomplish required cybersecurity training
- Clearly defined personnel actions if there are failures to meet the terms for employment
- Enterprise wide reporting on successful and non-successful cybersecurity activities from all levels of employees (develop a fun competitive environment)
- Build a program where everyone receives rewards i.e. time off or pizza party, when poor cybersecurity performance was avoided for a determined amount of days

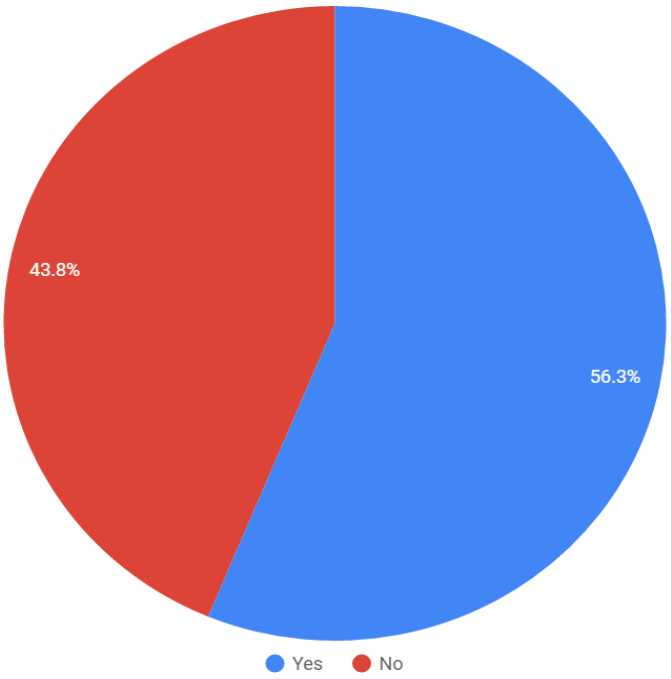

Figure 9: Survey participants with an engaged senior leadership regarding cybersecurity.

In conclusion, to make the most effective use of cybersecurity resources and to deliver swift incident response capabilities, organizations must raise awareness and showcase the risk reduction to all stakeholders within the enterprise. Once the groundwork and policies are in place incident response planning and execution will be an extension of the organization's business processes and culture.

4 - TRAINING AND EXERCISES

Summary

The objective behind exercises is to enable organizations to simulate emergency situations while also determining where they can make improvements. Exercises require participation and are designed to foster cross team discussions among participants to ensure roles and responsibilities are clarified before the real event occurs.

Gap #1: Tabletop Exercises Exist but Majority Don't Have Participation

Out of the 48 organizations surveyed, 38 (79%) are aware of tabletop exercises. However, out of those 38, only 18 organizations actually participate in tabletop exercises. This translates to only 38 percent of organizations participating in tabletop exercises. Without exercising incident response and disaster recovery plans in a simulation, organizations will not understand their pitfalls, shortcomings, and their efficacy until it is too late.

Inversing the participation rate, 62 percent of organizations that took the survey do not participate in tabletop exercises. Participation is lacking due to two main reasons: time and support. Senior leadership must dedicate the time and resources needed to perform a thorough organizational exercise. In regards to the industry breakdown, government and education have the biggest gap in participation. The government and education survey results reflected 71 percent and 72 percent, respectively, had no tabletop participation. If something were to happen, these organizations would have difficult time in responding swiftly and effectively.

Out of the organizations with 1-99 employees that took the survey, three out of the four organizations stated that they do not perform awareness training or have tabletop exercises. It is difficult for smaller organizations to tackle security because of the dedicated resources required.

Recommendation: Increase Participation

Include tabletop exercises as part of your security awareness training for key participants that are needed. Organizations that already have security awareness programs have the attention of their employees on the importance of completing or participating in the awareness program. Transitioning the awareness program to interactive exercises will provide a different take on an awareness program, while keeping participants interested. In addition, when including tabletop exercises within an already-established organization, the cost and personnel overhead should be minimal.

One suggestion would be for government and education to partner with members in the financial industry or stay in their industry and partner with others who have participation. This concept would also work with organizations that are lacking resources to orchestrate tabletop exercises.

Tabletop exercises should be performed at least once to twice a year, and each scenario should be different and incorporate lessons learned from the previous exercises. Scenarios could include, but are not limited to: insider threats; a breach (accidental or intentional); distributed denial of service attacks; and natural disasters.

Gap #2: Gaps in Awareness Training

The survey showed a consistent trend of various cybersecurity awareness training topics; Passwords (72%), Email Security (68%), Phishing (64%) and Web Security (60%). These are good topics that need to continue since these are the most common attack vectors impacting organizations. In addition, almost every organization that has been breached has been breached with user credentials. The following security awareness topics fell below 40 percent; Public Wi-Fi (38%), Mobile Security (32%), Travel Security (28%) and Media Handling (23%).

Recommendation: Ensure the Security Awareness Training has a Personal Touch

As we see ransomware attacks increase, we have to do more than train our end users on email and phishing campaigns. End users need to be fully engaged in active assessments of their readiness. Attack surfaces such as public Wi-Fi and media handling continue to be problematic for many organizations. Public Wi-Fi is convenient and attackers know this.

Organizations need to educate and provide their end-users with the knowledge and the tools to protect their Internet connections. In regards to media handling, many organizations still suffer from users trusting unknown external storage devices and plugging them into computers. In a different light, many end users may not know the risk involved in storing sensitive information on external storage devices or the security controls that may be available to them.

A recent attack surface that is becoming more common is the mobile device. As all industries continue to move more to mobile, the primary device for communication and storing data is a phone or tablet. Key business processes will be relying on the security and management of these devices. Validating the authenticity of the apps residing on these devices will be critical for ensuring the confidentiality, integrity and availability of data and the continuity of business.

End users need to have continuous education and training that is relevant to today's world. When creating the training, make it personal by explaining their responsibility within the organization. The end user is the first and last line of defense in many cases.

A lack of personnel is a common answer on why many organizations haven't been able to advance their cybersecurity posture. Organizations have the ability to be creative with resource management like partnering with others in their community and sharing knowledge regarding exercises. When people collaborate they are able to share success stories and failures that others can learn and build upon. In addition, by communicating with others, channels of communication are opened allowing for future collaboration and assistance during times of need.

5 - HARDENING CRITICAL INFRASTRUCTURE

Summary

For the analysis of critical infrastructure (CI), the Missouri Cybersecurity Task Force took a different approach than the common gap analysis. The Task Force engaged in a general assessment and how the results affected the continuity of government and health and human safety.

The Department of Homeland Security (DHS) designated 18 industries as critical infrastructure. This categorization reflects the fact that the compromise of any of these industries could pose significant threats to the well-being of the nation or human life. These industries also have many inter-dependencies making the security and health of each co-dependent in many situations on the collective security and operational health across this group. We utilized the DHS organization definitions of critical infrastructure areas and came up with the following:

- Water and Waste Water
- Power
- Communications and Federal Government Information Connections
- First Responders
- Military – National Guard
- Healthcare
- Transportation - Airports

To accomplish the assessment, the Task Force focused on each of the critical infrastructure areas and executed the first steps of the NIST 800-30 to perform the assessment. NIST 800-30 is a government approved assessment for determining cybersecurity risk on a system.

Our assessment has shown no significant gaps in any specific critical infrastructure, but various issues were identified. Our recommendations address each CI's issues and the issues each CI faces from other critical infrastructures they depend on. Finally, these CI to CI assessments and general risk profiles were combined to form recommendations that specifically deal with how the CIs affect the continuity of government and health and human safety.

Gap #1: Water and Power

Three municipalities and an independently owned utility were contacted directly by the Task Force. One additional survey respondent provided information. Out of the four total, three were energy only and two had both water and energy management.

From an energy standpoint, all providers are subject to the North American Electric Reliability Corporation (NERC) which has rigorous criteria for critical infrastructure protection (CIP). There are two major classifications of information held by utilities, customer data and energy management systems (control).

The sensitive information in customer data is concerned with confidentiality and privacy; customer energy usage data is considered sensitive information by some utilities in keeping with the NIST Internal/Interagency (IR) 7628 (Security and Privacy for the Smart Grid Volume II) guidelines.

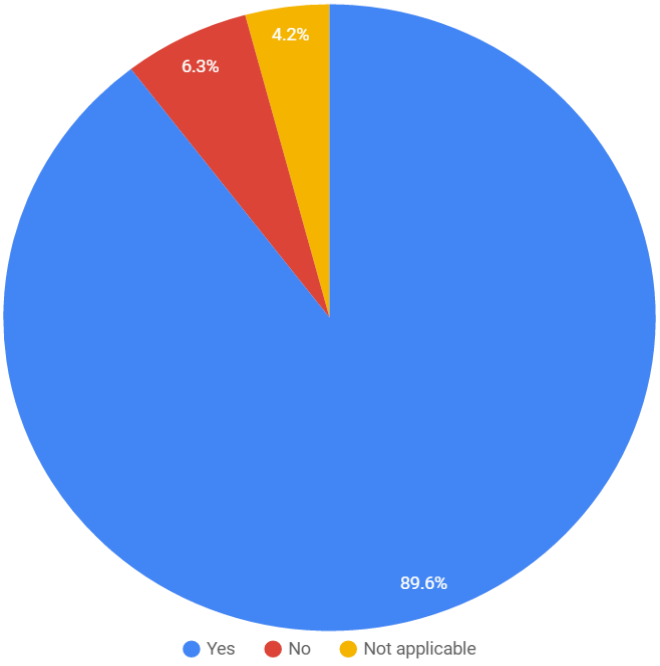

Figure 10: Survey participants with critical infrastructure

From an integrity point of view, the primary concern is protecting and ensuring proper billing. However, for public utilities some felt that confidentiality was not a concern since customer data availability is governed by state sunshine laws.

In control systems, availability of the data and systems is vital, and as such, the primary concern is maintaining operation. While there is some concern about confidentiality of this data, that aspect of data security is not as important operationally. For integrity, it's vital that no bad signals are presented to switching equipment and that data being received from the control system is correct and unaltered.

Threats for both data types are monitored through clearinghouses including the NERC-CIP alert system and fusion centers and vulnerabilities are patched quickly. Two shortcomings were identified. One is that access to fusion center information requires a Top Secret (TS) clearance. As such, critical reports may not be available to be distributed in a timely fashion unless the utility employs a TS-cleared professional and has a secure conference facility (SCF). One utility reported that they did not have access to a full time cybersecurity professional to track threats.

In addition, ISACs are forums organized by critical infrastructure sectors in which a centralized collection of intelligence and events occur and are then distributed to subscribed industry members of that forum. Within the Electricity ISAC (E-ISAC), there is also a Cybersecurity Risk Information Sharing Program (CRISP) in which passive sensors called information-sharing devices (ISDs) are installed on participants' networks and send encrypted data to a CRISP analysis center operated by the Pacific Northwest National Laboratory (PNNL), which analyzes the data and sends alerts and mitigations measures to CRISP participants through a secure network. CRISP is a public-private partnership whose purpose is to facilitate timely information sharing of cybersecurity threat information and to develop situation awareness tools that enhance the electricity sector's ability to protect its critical infrastructure. CRISP also provides the ability to look across organizations within the electricity subsector to identify correlation and trends.

Water security does not have stringent standards as energy, for those two utilities surveyed. The security culture was heavily influenced by the NERC CIP standards from energy. A source of threat analysis could be from the State of Missouri. Water control is seen as relatively primitive with remote operation of valves over serial connections. Water risk assessments are not performed on a regular basis.

For both infrastructures (energy and water) security boundaries were correctly drawn, preventing writing, from the enterprise business network into the supervisory control and data acquisition (SCADA) network. SCADA networks are typically firewalled off from business networks, often established on separate sub-networks to protect the operational and data integrity of these critical systems. In one case, reading from the SCADA network was an offline/download process used solely for system analysis. Energy management control systems are a focal point of the NERC CIP standards, with stringent cybersecurity requirements assessed to protect the electrical grid.

The threat likelihood for all surveyed was seen as surprisingly low. To quote one source "we are such a small operation, that we do not feel we are on anyone's radar". Both CI have to be on guard to protect against typical cybersecurity threats that can be exploited to potentially compromise business and operational control systems. Without continual due diligence in applying defense in depth layers of security, both CI would be significantly impacted by common threats.

An increasing number of breaches are occurring at the hands of compromised third party credentials. Attention must be given to the diligent management of third party supplier credentials, including the use of multi-factor authentication to protect against loss of mishandled credentials. Additionally, the level of sophistication behind cyber-attacks has grown significantly with threat actors becoming much stealthier and also using a combination of attack methods in some cases to achieve their goals.

The attack on the distribution system of an electric utility in Ukraine last December, which was the first confirmed case of a blackout at the hands of a cyber-attack, actually began as a spear-phishing attack. Over time as the attackers probed

deeper into the environment, a variety of methods were used to steal credentials and eventually execute an attack that consisted of multiple attack methods including exploiting stolen credentials. The attackers had remote access control of the distribution controls, leveraged destructive firmware rewrites of communication devices in substations, and a telephony denial of service attack to block the use of telephony.

The increasing complexity of attacks and stealthy tactics by threat actors must continue to be mitigated through increasingly effective cybersecurity awareness programs on the part of these industries to educate their employees against these risks.

It was generally understood that lack of control of the energy and water systems could be detrimental to society. Specifically, lack of energy distribution control can cause system blackouts, frequency instability, and potentially equipment destruction. The power industry is generally regarded as sitting atop the critical infrastructure "food chain" based upon the many operational, health, and well-being dependencies of other critical infrastructure industries on power, hence the stringent requirements on this industry group. In water, contamination and outages were seen as issues. Specifically, in water, running a pump dry could prevent distribution of clean water to large parts of the service area for a significant amount of time.

Recommendation: Raise Awareness and Increase Information Sharing.

There needs to be greater awareness and appreciation of the growing cybersecurity threats to critical infrastructures. In all cases, the likelihood of the threat was seen to be very low, even for purely physical attacks, where much of the concentration was focused for several utilities. Customer data collected by the utilities could potentially violate personal privacy and/or HIPPA regulations if divulged. Fusion center information needs to be able to be downgraded quickly to reach utilities in a timely fashion to enable meaningful action. The sharing of best practices and access to early research performed within the state could benefit greater understanding of threats to these cyber-physical infrastructures.

Gap #2: Communication and Fusion Centers

Fusion Center

Background: National fusion centers provide actionable intelligence for state and local authorities and include participation from industry and the private sector. The scope of the work at the national fusion centers includes terrorism, criminal and public safety matters. In the area of public safety and within the charter of monitoring and protecting critical infrastructure, the national fusion centers is a valuable information resource for this project but may also be able to provide some solutions and/or help fill some of the identified gaps.

For purposes of our project, we have aligned national fusion centers with the "communications" function of critical infrastructure. Although, as a potential solution for gaps, this may be a bit narrow, the fusion center does indeed provide its key service of state and local situational awareness based on its communications capability.

Fusion centers are a part of both the problem space and a potential solution to the cybersecurity challenges faced by critical infrastructure. It can be argued that each function within fusion Centers is only as good as the ability of the different elements of law enforcement and public safety sectors to report

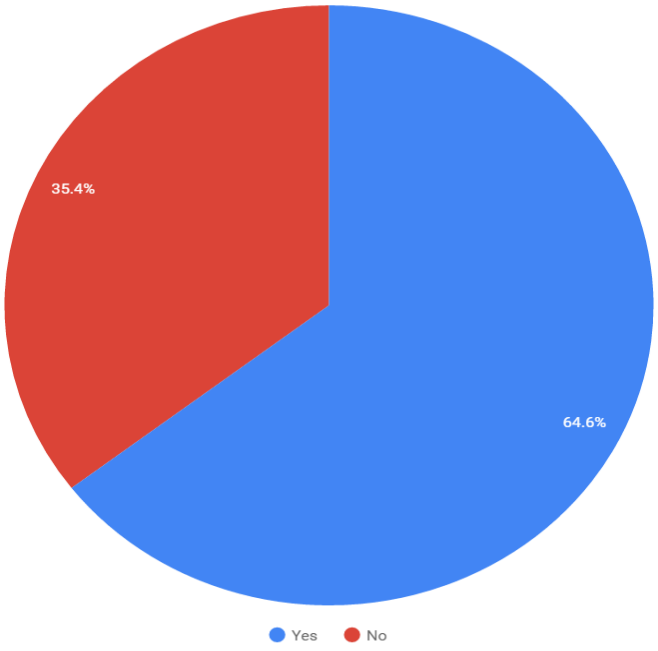

Figure 11: Survey participants that perform security assessments

the current situation. While the communications infrastructure is one of many pieces of national infrastructure that the fusion center helps to protect, it also depends on communications systems. Because even unclassified information that is useful for preparing protections is time-sensitive, any delay or breakdown in the communications systems and processes inhibit the ability of critical infrastructure to either prepare or respond.

The breakdown in communications doesn't necessarily mean a direct result of a cybersecurity attack but could be a secondary effect. For example, it would be preferred if a utility company having threat or vulnerability issues could share that with other utility companies around the country through fusion centers. However, if the attack is a cybersecurity threat impacting communications, such as the victim organization's ability to log, monitor and report its situation, it may not even be aware of the attack let alone have the ability to communicate the details.

Interoperability is also a challenge in communication for critical infrastructure that needs to benefit from national resources such as the fusion center. At the most fundamental level, the different industries that make up critical infrastructure don't always speak the same language. Concerning cybersecurity threats and vulnerabilities, these concepts are relatively new to some industries making common language even more difficult. Many key components of critical infrastructure are based on legacy SCADA systems sometimes called "industrial control systems." Designing and operating SCADA systems is a fairly new concept within cybersecurity. Very few cybersecurity evaluation standards exist that are common to critical infrastructure using SCADA systems. Therefore, reporting and/or using cybersecurity threat intelligence information and taking action on such information becomes challenging.

Lastly, as it relates to communication, fusion centers have reached out to industry in order to apply context to the information shared with its participants. Communicating risks and particularly the impact of cybersecurity threats requires the context and potential consequences that are best measured by experts in those particular industries that make up critical infrastructure. For example, a serious cybersecurity threat associate with a particular vulnerability in one industry, may be somewhat "normal" in another.

Communications

The Task Force interviewed a large telecommunications company to obtain the assessment on Missouri communications. We found that the company is quite robust in preparation for cybersecurity attacks as it is the number 3 target for cyber-attacks behind #1 – the military, and #2 – the financial industry. This means that cybersecurity is a top priority for them. Cybersecurity vigilance is front and center and a requirement for the success of their business. As much as they could tell us, they have a vast network of redundancies and backups, separated from each other and capable of backfilling either if they become compromised. They also have extensive hardening on these systems. To ensure their customer's protection, they have to provide significant cybersecurity protection and services as a basic level of coverage as part of their customer service level agreements.

Recommendation: Fusion Center

A potential way to better leverage national resources such as fusion centers is to create a public private partnership that facilitates coordination, standards, awareness and communication between the institutions (people, processes and technology) that comprise critical infrastructure. Some quick and perhaps low cost options that may require further investigation include:

- Take advantage of the fusion centers Located in St. Louis, Kansas City, and Jefferson City
- Explore better ways to communicate cybersecurity threat, vulnerabilities and potential solutions between those organizations that comprise critical infrastructure. Do this through:
    - The National Council of ISACS http://www.nationalisacs.org/
    - Align with an existing ISAC http://www.nationalisacs.org/member-isacs
    - Consider forming a new ISAC in sectors where none exists
- Consider leveraging the National Critical Infrastructure Coordination Center (NCICC) https://www.dhs.gov/national-infrastructure-coordinating-center

- Look for ways to obtain funding through the Presidential Directive for Protection of Critical Infrastructure (PPD-21).
- NOTE: Most information from fusion centers carry a classification level. Some thought will need to be given to this as to how the State of Missouri will partner with them.

Recommendation: Communications

Ensure that the government and the CIs that are heavily dependent on communication (first responders, energy, and healthcare) employ landline redundancies and establish considerable backup plans that can involve mobile units. Also, the government emergency communication systems need to have redundant communication systems. These systems include but not limited to Amber Alert and emergency broadcast systems.

Gap #3: First Responders and National Guard

First Responders

After surveying some local law enforcement agencies, it was found that all have risk to their internal computer networks via the use of email. The primary threat of exposure of the network to malware attacks comes specifically from email and email attachments. The malware comes in a variety of different formats. Law enforcement organizations are targeted by ransomware attacks quite heavily. The infection of department networks and directories by malicious software can bring IT infrastructure to a standstill. Even if the malware is detected the infected area would be taken offline for repair. The time that equipment was offline would mean a stoppage of operations and service delivery.

National Guard

The national security mission of the Missouri National Guard (MONG) demands a fair amount of cybersecurity resilience. The MONG is hardened with regards to port entry and external threats to protect its mission readiness and ability to support the State of Missouri and the Department of Defense (DoD) in various missions. However, for internal intrusion or access from phishing, emails, or sneaker net introduced threats, there is still work to be done to protect human introduced issues. All that remains is to have more cybersecurity hygiene. General hardening is mature for the MONG, and they are prepared to assist in any number of cybersecurity issues through their cybersecurity team and its efforts to support Title 10 and Title 32 order and missions.

Recommendation: First Responders

To maintain the critical systems of the first responders so as to support continuity of government and health and human safety some basic cybersecurity hygiene and continued hardening is essential. To that end, here are the following recommendations:

- Additional training of personnel regarding the use of email and the internet
- The use of email filtering systems and firewalls
- The use of backup generators for power loss
- The establishment of a secondary business continuity site on a separate power circuit infrastructure and on a separate C.O.
- Using a network mesh to make loss of connectivity difficult. A network ring can also be beneficial
- Data redundancy and emergency services system redundancy

Recommendation: National Guard

While the MONG is ready to assist with its incident response capabilities it needs assistance with governance, oversight, and funding. The path to leverage MONG's cybersecurity capabilities is currently complex, especially for any private organization that would like to leverage their capabilities. It is possible that through agreed upon MOUs established before an event occurs, many of the issues in leveraging the MONG become moot. The State of Missouri Office of Administration for instance, has an MOU in place with the MONG that defines roles and responsibilities in the event cybersecurity incident response is requested.

The MONG has a focus on health and human safety that has been demonstrated successfully again and again all over the state in dealing with natural disasters and other emergencies. Any disaster relating from a cybersecurity incident, the MONG can and should be there to assist human safety.

Gap #4: Healthcare

Medical networks are critical infrastructure that people utilize for all cases of wellness and health issues. Medical networks have significant technologies that enable automation from very simple repetitive tasks to highly critical patient care.

One of the findings within the survey and from talking to organizations is that multiple IT ecosystems typically exist within a healthcare provider. The different infrastructures are the patient information infrastructure, the communication infrastructure, the power infrastructure for emergency power, the healthcare monitoring infrastructure, the blood bank IT infrastructure, and the infrastructure for drug dispensation. All these ecosystems work in sync, and failure of one typically is overcome by manual intervention whenever possible. One of the important gaps while evaluating this infrastructure is the lack of comprehensive processes driven by risk analysis. Not all the practitioners of these IT ecosystems are appropriately trained on cybersecurity related risks. It is therefore required that the state provide the avenues and the encouragement that all IT personnel be trained in understanding risk within the NIST guidelines. The complexity of such an ecosystem can be difficult to comprehend.

Recommendation: Healthcare

All of the dissimilar ecosystems within a healthcare organization have difficulty talking with one another as their data formats are generally incompatible. It is recommended that a common data format be developed in collaboration with the research entities and be adopted. Another recommendation is to partner with the DHS offices to come up with proper risk analysis and mitigation frameworks. Also another recommendation is a mandatory risk analysis training of workforce involved in the healthcare critical infrastructure.

The Task Force recommends that the government work with the healthcare industry to ensure rigidity in its cybersecurity practices to make sure that during a cybersecurity attack, the healthcare systems will be available to function. NIST is working on a healthcare cybersecurity framework that would be good to enforce for the healthcare systems; however, Healthcare Information Management Systems Society (HIMSS) has recommended that NIST make it voluntary to ease acceptance. The State of Missouri will have to weigh this carefully.

Health information, logistics, and treatment records are critical to health and human safety and are vulnerable to cybersecurity attacks. Additionally, there is a considerable drug trade that comes from tampering with medical records so protecting this aids in the prevention of prescription drug abuse which is becoming a larger and larger problem every year. Ensuring strict cybersecurity standards, training, exercises, and other tactical experiential learning will ensure that our healthcare professionals are as proficient as possible. This is a real opportunity for Missouri to set a new standard of healthcare excellence with a robust and iterative security training and posture for its word class healthcare institutions.

Gap #5: Transportation

The Task Force assessed one significant airport within Missouri. The airport has done a very good confidentiality, integrity, and availability analysis on all of their data sources with an outside consultant.

Recommendation: Airports

Airports are critical to move society forward and the economy of our state. We can have limited function without airports in times of emergencies, but without them, day to day life would be difficult and there would be considerable economic challenges.

As such, ensuring these transportation hubs remain secure is critical to the health of our state. We recommend ensuring full compliance with cybersecurity recommendations from the National Institute of Standards and Technology (NIST),

National Cybersecurity Center of Excellence (NCCoE), and DHS. The Transportation Security Administration (TSA) makes the adoption of the NIST cybersecurity framework voluntary, but the State of Missouri should consider making it mandatory for Missouri's large airports.

The State of Missouri should consider encouraging and supporting these collaborations to strengthen the security of these travel hubs and to bring further credit to the efforts of Missouri being a leader in cybersecurity.

CONCLUSION

While many organizations across the State of Missouri have made great strides in hardening their cybersecurity posture and raising awareness, as covered within this plan, there is still a lot of work to accomplish. Small organizations, in particular smaller local governments and schools, have an uphill battle for resources, namely funding and personnel. All organizations must continue to strive to raise cybersecurity awareness levels and understand what is at risk. When awareness is entwined within the day-to-day activities, it empowers all employees to become the first and last line of defense and assists with identifying risk. By knowing what is at risk, organizations can make intelligent investments and business process changes to make themselves more resilient to an attack.

PRIMARY RECOMMENDATIONS

1. **Identify Organizational Risk:** Many processes and technologies leveraged by an organization have vulnerabilities. However, without identifying what is at stake and determining the likelihood of exploits being successful, an organization will be wandering in the dark attempting to harden itself against cybersecurity attacks. One of the best methods of quickly identifying organizational risk is through the use of table top exercises and other self-driven risk assessments.
2. **Raise Awareness:** Raising organizational awareness about the identified risks and threat actors is paramount in today's environment. Individuals are targeted in their personal and professional lives, and arming our citizens and employees with the proper knowledge is key to personal safety as well as to their employer's cybersecurity posture.
3. **Leverage Existing Resources:** Organizations should not reinvent the wheel nor should they go out on their own necessarily in acquiring or implementing security controls. The organization's industry ISAC, various peers, and the State of Missouri can assist in maximizing existing contracts and support of existing cybersecurity frameworks and best practices.
4. **Support STEM:** Increasing the desire of STEM within tomorrow's workforce will play a pivotal role in protecting critical infrastructure and business processes. K-12 and higher education need to continue to engage students on the possibilities of where STEM can take them; professional development centers need to assist, coordinate, and develop programs for individuals both trying to get into the cybersecurity field and others trying to further their career; and mature organizations need to further their internship programs to help foster tomorrow's workforce.